IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Original): A wireless communication device, comprising:

a wireless communication unit which communicates with other communication device located at a prescribed range;

a first identification information generator which generates first identification information including a service name of available service and inherent information;

an encryption unit configured to encrypt said first identification information by using a prescribed encryption key to generate encryption data;

a second identification information generator which generates second identification information including the service name, the inherent information and the encryption data; and

an inherent information transmitter which transmits the second identification information for an other communication device which has requested transmission of the inherent information.

Claim 2 (Original): The wireless communication device according to claim 1, wherein said first identification information generator uses a Hash value obtained by a Hash operation for data including the service name and the inherent information, as said first identification information.

Claim 3 (Original): The wireless communication device according to claim 1, wherein said second identification information generator generates the second identification information in which the encryption data is arranged after the service name, and information indicative of a length of the service name is arranged before the service name.

Claim 4 (Original): The wireless communication device according to claim 1, wherein said second identification information generator generates the second identification information in which information indicative of whether or not check of reliability is necessary is arranged before information indicative of a length of the service name.

Claim 5 (Original): The wireless communication device according to claim 1, wherein said wireless communication unit communicates with the other communication devices by P2P (Peer to Peer).

Claim 6 (Original): The wireless communication device according to claim 1, wherein said encryption unit encrypts again the first identification information to generate the encryption data, when an expiration data of the encryption key passes.

Claim 7 (Original): A portable terminal, comprising:

a wireless communication unit which communicates with other communication devices located at a prescribed range;

a search unit configured to search the other communication devices capable of communicating;

an identification information acquisition unit which acquires first identification information transmitted from the searched communication device;

an information extracting unit configured to extract a service name, inherent information and encryption data from the acquired first identification information;

a decryption unit configured to decrypt the encryption data by using a prescribed decryption key;

a comparison unit configured to compare the decrypted data with the service name and the inherent information extracted by said information extracting unit, and to determine whether or not the other communication device searched by said search unit is reliable; and

a communication controller which inhibits communication with the communication device determined to be unreliable by said comparison unit.

Claim 8 (Original): The portable terminal according to claim 7, further comprising:

an information indicating unit which indicates to users information indicative of being unreliable when users try to connect to the communication device determined to be unreliable by said comparison unit.

Claim 9 (Original): The portable terminal according to claim 8, further comprising:

a list register unit configured to register a list of the other communication devices determined to be unreliable by said comparison unit;

wherein said communication controller inhibits communication with the communication devices registered to said list register unit.

Claim 10 (Original): The portable terminal according to claim 7, wherein said identification information acquisition means extracts data of a first length from a head of the information transmitted from the communication device searched by said search unit, and determines whether the information is the first identification information based on the extracted data.

Claim 11 (Original): The portable terminal according to claim 10, wherein said information extracting unit extracts data of a second length from a head of the first

identification information, and decides a length of the service name based on the extracted data.

Claim 12 (Original): The portable terminal according to claim 11, wherein said information extracting means extracts data of a length of the decided service name from a head of data except for data of the first and second lengths from a head of the first identification information, as the service name.

Claim 13 (Original): The portable terminal according to claim 12, wherein said information extracting unit extracts data of a third length from a head of data except for the first length, the second length and the length of the decided service name from the head of the first identification information, an inherent information.

Claim 14 (Original): The portable terminal according to claim 13, wherein said information extracting means determines whether or not data except for the first length, the second length, the length of the decided service name, and the third length from a head of the first identification information is a fourth length, and if the data is the fourth length, extracts the data as the encryption data.

Claim 15 (Original): The portable terminal according to claim 7, further comprising a Hash operation unit which performs a Hash operation for data including the service name and the device identification name extracted by said information extracting unit to generate a Hash value,

wherein said comparison unit compares the decoded data with the generated Hash value.

Claim 16 (Original): The portable terminal according to claim 7, wherein said wireless communication means communicates with the other communication devices by P2P (Peer to Peer).

Claim 17 (Original): The portable terminal according to claim 7, wherein said decoder decodes the encryption data by using a new decryption key when an expiration date of the decryption key passes.

Claim 18 (Canceled).

Claim 19 (Previously Presented): A computer readable medium storing a computer program code which controls a portable terminal, to perform controls comprising:

communicating with other communication devices located at a prescribed range;

searching a communication device capable of communicating;

acquiring first identification information transmitted from the searched communication device;

extracting a service name, inherent information and encryption data from the acquired first identification information;

decrypting the encryption data by using a prescribed decryption key;

comparing the decoded data with the extracted service name and inherent information, and determining whether or not the communication device searched by the searching unit is reliable based on the comparison result; and

inhibiting communication with the communication device determined to be unreliable by the comparison result.

Claim 20 (Original): A communication system comprising a portable terminal and a wireless communication unit capable of communicating with said portable terminal located at a prescribed range,

wherein said portable terminal includes:

a searching unit configured to search a communication device capable of communicating;

an identification information acquisition unit configured to acquire first identification information transmitted from the searched communication device;

an information extracting unit configured to extract a service name, inherent information and encryption data from the acquired first identification information;

a decryption unit configured to decrypt the encryption data by using a decryption key prescribed in advance;

a comparison unit configured to compare the decrypted data with the service name and the inherent information extracted by said information extraction unit, and determines whether or not the communication device searched by said searching unit is reliable; and

a communication controller which inhibits communication with the communication device determined to be unreliable by said comparison unit,

said wireless communication unit includes:

an inherent information acquisition unit configured to acquire the inherent information;

a first identification information generator which generates first identification information including the service name and the inherent information;

an encryption unit configured to encrypt the first identification information by using the encryption key prescribed in advance, and generates the encryption data;

a second identification information generator which generates second identification information including the service name, the inherent information and the encryption data; and

an inherent information transmitter which transmits the second identification information for the other communication device which has requested transmission of the inherent information.